UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/789,311	02/27/2004	Sheueling Chang Shantz	6000-31500	9201

58467 7590 02/15/2008

MHKKG/SUN
P.O. BOX 398
AUSTIN, TX 78767

EXAMINER	
JOHNSON, CARLTON	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
02/15/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Ak

Advisory Action **Before the Filing of an Appeal Brief**	**Application No.** *10/789,311*	**Applicant(s)** SHANTZ ET AL.
	Examiner Carlton V. Johnson	**Art Unit** 2136

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 28 January 2008 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

a) ☒ The period for reply expires 3 months from the mailing date of the final rejection.

b) □ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. □ The Notice of Appeal was filed on ____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. □ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because

(a) □ They raise new issues that would require further consideration and/or search (see NOTE below);

(b) □ They raise the issue of new matter (see NOTE below);

(c) □ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or

(d) □ They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: ____. (See 37 CFR 1.116 and 41.33(a)).

4. □ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).

5. □ Applicant's reply has overcome the following rejection(s): ____

6. □ Newly proposed or amended claim(s) ____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

7. ☒ For purposes of appeal, the proposed amendment(s): a) □ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.

The status of the claim(s) is (or will be) as follows:

Claim(s) allowed: ____.

Claim(s) objected to: ____.

Claim(s) rejected: *1-67*.

Claim(s) withdrawn from consideration: ____.

AFFIDAVIT OR OTHER EVIDENCE

8. □ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).

9. □ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).

10. □ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.

12. □ Note the attached Information Disclosure Statement(s). (PTO/SB/08) Paper No(s). ____

13. □ Other: ____.

Continuation of 11. does NOT place the application in condition for allowance because:
Response to Arguments

The 101 rejection will be upheld due to the fact that the claim limitations indicate arithmetic operations which are used to perform cryptographic calculations. The claim limitations mention a public-key cryptographic application. But, there is no indication in the specification or original claims that the only operations performed by the public-key cryptographic application are arithmetic operations for cryptographic calculations. Applicant states that the cryptographic calculations implement a portion of a cryptographic application. (Remarks Page 6, Lines 24-26) It is well known in the art that a cryptographic application performs more functions than arithmetic operation for cryptographic calculations.

Citations cited in Office Action indicate arithmetic operations equivalent to arithmetic operations performed in claim limitations. The Gressel and Stribaek prior art combination discloses arithmetic operations performed on integer values. The stated types of operations indicated by the prior art discloses addition, multiplication, XOR operations, and etc.

The Gressel prior art discloses arithmetic operations such as multiplication and addition utilizing partial results of the first operation. The Gressel prior art discloses the results of a first arithmetic operation used as input to another arithmetic operation. (see Gressel col. 3, lines 1-7; col. 53, lines 13-19; col. 53, lines 49-51: feedback of a previous operation into next operation; col. 2, lines 31-37: multiplication two values, summing two values utilizing partial (i.e. bit operations, any bit length, high order bits, low order bits) results from previous multiplication) A partial result is a value of having a bit length less than the total bit length of a word. The high order bits are a partial result. The low order bits are a partial result. In addition, the Stribaek prior art discloses the selection of high order bits and/or low order bits in arithmetic operations. (see Stribaek col. 7, lines 3-5) This is equivalent to a first partial result representing the high order bits summed with the low order bits of a result of a first number multiplied by a second number.

The referenced prior art discloses the generation of a partial result, the usage of that partial result in subsequent arithmetic operations. (see Stribaek col. 7, lines 3-5) The referenced prior art discloses a complete set of the types of arithmetic operations disclosed in the claims limitations (XOR operation, multiplication, carry add operations, carry save operations) The Office Action indicates citations for each independent and each dependent claim rejection.

In very long instruction word (VLIW) architectures, which include many microcode architectures, multiple simultaneous operations and operands are specified in a single instruction. (http://www.answers.com/topic/instruction-computer-science) This standard computer architecture feature discloses a single arithmetic instruction to perform multiple arithmetic operations.

An instruction also designates the destination address (memory locations, registers) for the results of the completion of an instruction. ("On traditional architectures, an instruction includes an opcode specifying the operation to be performed, such as "add contents of memory to register", and zero or more operand specifiers, which may specify registers, memory locations, or literal data ": http://www.answers.com/topic/instruction-computer-science)

The examiner has considered the applicant's remarks concerning In response to executing an arithmetic instruction, a first number is multiplied by a second number, and a partial result from a previously executed single arithmetic instruction is fed back from a first carry save adder structure generating high order bits of the current arithmetic instruction to a second carry save adder tree structure being utilized to generate low order bits of the current arithmetic instruction to generate a result that represents the first number multiplied by the second number summed with the high order bits from the previously executed arithmetic instruction. Applicant's arguments have thus been fully analyzed and considered but they are not persuasive.

After an additional analysis of the applicant's invention, remarks, and a search of the available prior art, it was determined that the current set of prior art consisting of Gressel (6,748,410) and Stribaek (7,181,484) discloses the applicant's invention including disclosures in Remarks.

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

2/11/08